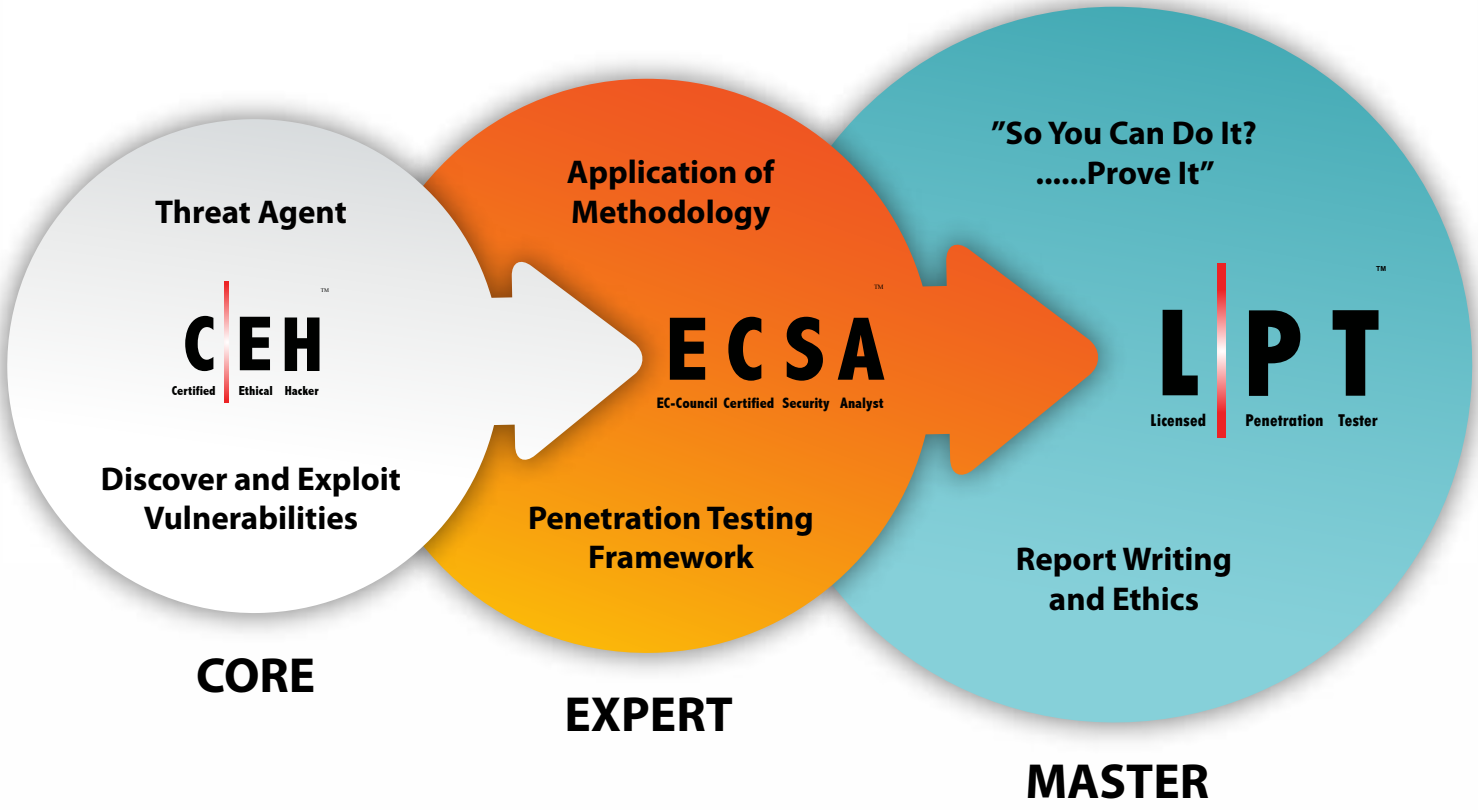

Analyze. Secure. Defend.
Do you hold ECSA credential?
ECSA™
EC-Council Certified Security Analyst
EC-Council
Hackers are here. Where are you?

EC-Council Cyber Security Professional Path



EC-Council Certified Security Analyst (ECSA)

What is the EC-Council Security Analyst program?

You are an ethical hacker. In fact, you are a Certified Ethical Hacker. Your last name is Pwned. You dream about enumeration and you can scan networks in your sleep. You have sufficient knowledge and an arsenal of hacking tools and you are also proficient in writing custom hacking code.

Is that enough?

Can you become an industry accepted security professional? Will organizations hire you to help them protect their systems? Do you have any knowledge in applying a suitable **methodology** to conduct a penetration test for an enterprise client? Do you have any experience writing a custom penetration testing report?

More importantly, do you have a globally recognized certification that can verify your penetration testing capabilities?

If you are the person above, what you may be lacking is the knowledge and experience to execute a successful penetration test according to accepted industry standards.

The ECSA is a security credential like no other! The ECSA course provides you with a real world hands-on penetration testing experience and is a globally accepted hacking and penetration testing class available that covers the testing of modern infrastructures, operating systems and application environments while teaching the students how to document and write a penetration testing report.

The ECSA program takes the tools and techniques you learned in the Certified Ethical Hacker course (CEH) and elevates your ability into full exploitation by teaching you how to apply the skills learned in the CEH by utilizing EC-Council's published penetration testing methodology

It is a highly interactive, comprehensive, standards-based and methodology intensive training program 5-day security class which teaches information security professionals to conduct real life penetration tests.

This course is the part of the Information Security Track of EC-Council. This is a "Professional" level course, with the Certified Ethical Hacker being the "Core" and the Licensed Penetration Tester being the "Master" level certification.

The iLabs Cyber Range

As the ECSA course is a fully hands-on program, the exercises cover real world scenario. By practicing the skills that are provided to you in the ECSA class, we are able to bring you up to speed with the latest threats that organizations may be vulnerable to.

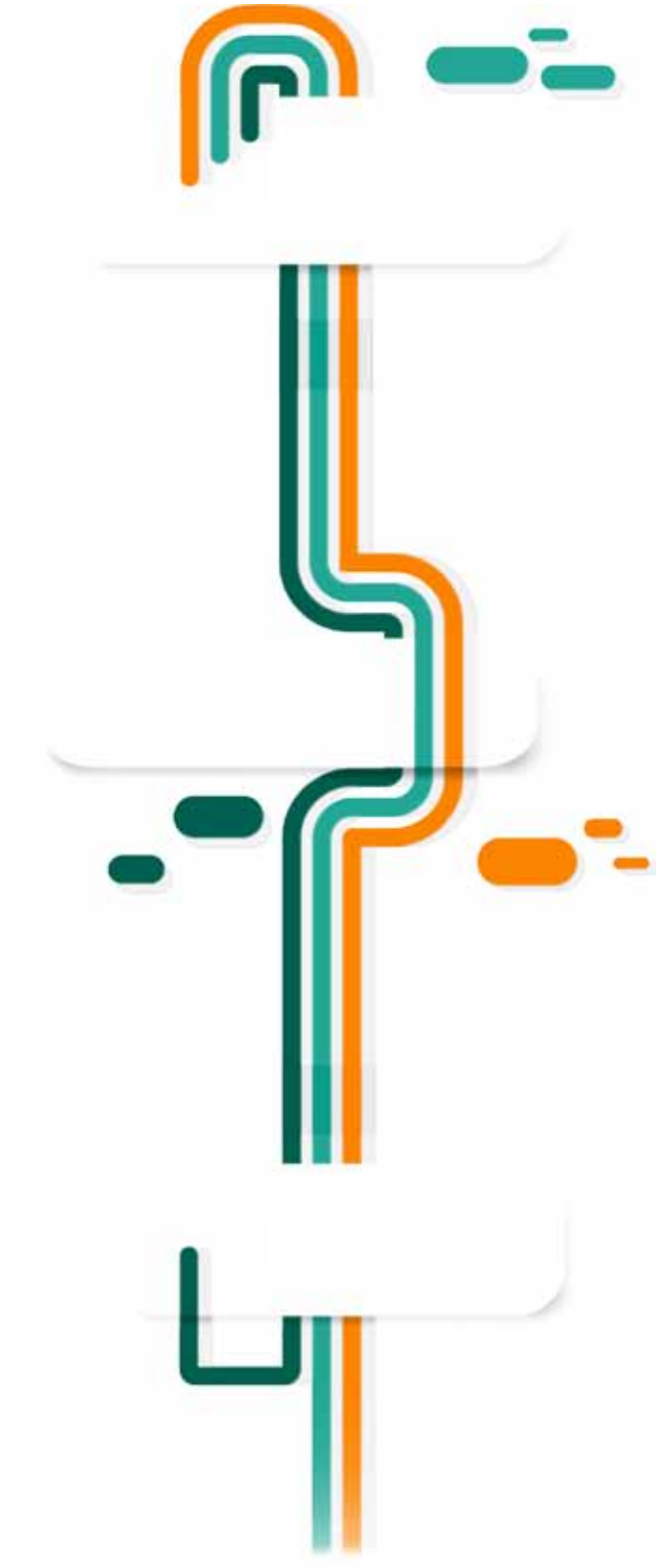
This can be achieved with the EC-Council iLabs cyber range. It allows students to dynamically access a host of Virtual Machines preconfigured with vulnerabilities, exploits, tools, and scripts from anywhere with an internet connection.

Our web portal enables the student to launch an entire range of target machines and access them remotely with one simple click. It is the most cost effective, easy to use, live range lab solution available.

With iLabs, lab exercises can be accessed 24x7 allowing the student to practice skills in a safe, fully functional network anytime it's convenient.

Our guided step-by-step labs include exercises with detailed tasks, supporting tools, and additional materials as well as our state-of-the-art "Open Environment" allowing students to launch a complete Live range open for any form of hacking or testing.

Available target machines are completely virtualized allowing us to control and reset machines quickly and easily with no required instructor or administrative interaction.



What's New in ECSA V9?

Skills Based Competency

The ECSAV9 penetration testing course is designed to enhance the skills based competency of a penetration tester. This course is intensively hands-on and a tremendous amount of emphasis is placed on the practical competency of the student.

Unlike the previous version of ECSA exam, in the new ECSAv9, a student will only be allowed to challenge the ECSA exam after meeting certain eligibility requirements.

To become eligible, a student must conduct a detailed penetration test through the EC-Council Cyber Range iLabs environment and submit a written report via EC-Council's ASPEN system.

Only candidates that successfully complete the penetration test in the Cyber Range iLabs environment are allowed to challenge the ECSA exam.

You will conduct a penetration test on a company that has various departments, subnets and servers, and multiple operating systems with defense mechanisms architecture that has both militarized and non-militarized zones.

The design of the course is such that the instructor in the class will actually take you through the core concepts of conducting a penetration test based on EC-Council's published penetration testing methdology and guide you through the report writing process for this organization.

Who Should Attend

Ethical Hackers, Penetration Testers Network server administrators, Firewall Administrators, Security Testers, System Administrators and Risk Assessment professionals.

Duration

5 days (9:00 - 5:00)

Certification Exam

The ECSA exam aims to test a candidate's knowledge and application of critical penetration testing methodologies.

The exam requires a candidate to perform real-world penetration testing over EC-Council's secure cyber-range and to produce a penetration testing report which clearly document the vulnerabilities found. This report will be graded by our professionals. Candidates that successfully submit an acceptable report will proceed on to a multiple choice exam that tests a candidates knowledge.

Candidates that successfully submit an acceptable report and the pass the multiple choice exam will be awarded the ECSA credential.

What is the Outline of ECSA?

Core Modules

1. Security Analysis and Penetration Testing Methodologies
2. TCP IP Packet Analysis
3. Pre-penetration Testing Steps
4. Information Gathering Methodology
5. Vulnerability Analysis
6. External Network Penetration Testing Methodology
7. Internal Network Penetration Testing Methodology
8. Firewall Penetration Testing Methodology
9. IDS Penetration Testing Methodology
10. Web Application Penetration Testing Methodology
11. SQL Penetration Testing Methodology
12. Database Penetration Testing Methodology
13. Wireless Network Penetration Testing Methodology
14. Mobile Devices Penetration Testing Methodology
15. Cloud Penetration Testing Methodology
16. Report Writing and Post Test Actions

Self-Study Modules

1. Password Cracking Penetration Testing
2. Router and Switches Penetration Testing
3. Denial-of-Service Penetration Testing
4. Stolen Laptop, PDAs and Cell Phones Penetration Testing
5. Source Code Penetration Testing
6. Physical Security Penetration Testing
7. Surveillance Camera Penetration Testing
8. VoIP Penetration Testing
9. VPN Penetration Testing
10. Virtual Machine Penetration Testing
11. War Dialing
12. Virus and Trojan Detection
13. Log Management Penetration Testing
14. File Integrity Checking
15. Telecommunication and Broadband Communication Penetration Testing
16. Email Security Penetration Testing
17. Security Patches Penetration Testing
18. Data Leakage Penetration Testing
19. SAP Penetration Testing
20. Standards and Compliance
21. Information System Security Principles
22. Information System Incident Handling and Response
23. Information System Auditing and Certification

Note: Self-study modules are available in ASPEN portal

GET CERTIFIED

ECSA v9 Exam Information

The ECSAv9 exam includes 2 required stages.

Report writing stage requires candidates to perform various penetration testing exercises on EC-Council's iLabs before submitting a pentest report to EC-Council for assessment. Candidates that submit reports to the required standards will be provided with exam vouchers for the multiple choice exam.

Multiple choice exams are proctored online through the EC-Council Exam portal or VUE:

Credit Towards Certification: ECSA v9
Number of Questions: 150
Passing Score: 70%
Test Duration: 4 hours

What Will You Do – The ECSA ASSESSMENT

The course comprises of 2 sets of lab challenges. Both are on the EC- Council ilabs Cyber Range.

The first set covers practise labs for each module. In all, there are 45 such labs in total.

The other is a Challenge Scenario which mimics an actual penetration test in an imaginary financial service company. As a pre-requisite, you will be required to actually complete a penetration testing activity and submit a report to EC-Council before you will be allowed to attempt the ECSAV9 Exam.

The Challenge Scenario

Brian works as a personal loan manager at FNB Financial Services which is a large multinational consulting corporation, headquartered in Atlanta, U.S.A. FNB specializes in personal, home equity, and debt consolidation loans around the world. Brian has been a trusted foot soldier for his organization for over a decade and is reeled in to handle only high-profile cases. Since Brian mostly telecommutes with his overseas clientele, he relies heavily on the network infrastructure of his organization.

Infrastructure Available to Brian

Like any large organization, FNB's internal network consists of several subnets housing various organizational units. The front office is connected to a separate subnet which connects to the company's public-facing computers. The company has installed various kiosks to help customers understand their product and services. The front office also has a Wi-Fi connectivity to cater users who carry their own smartphones and laptops.

The FNB's internal network is made up of Militarized and Demilitarized Zones connected with a huge pool of database servers in Database Zone. As a security precaution, and by design, all the internal resource zones are configured with different subnet IPs. The militarized zone houses the application servers that provide application frameworks for various departments of the organization.

The Demilitarized Zone contains public facing systems of the organization such as web and mail servers.

FNB headquarters' network topology and protocols are replicated around the world in all its satellite offices for easy communication with the headquarters.

Brian's Predicament

Brian is all set to present a loan consolidation plan to one of his biggest client from Japan. Mr. Takamashi, client's representative, has agreed for a video conference to go over and discuss Brian's proposal. Half an hour before the call, Brian switches on his laptop which is connected to the company's Wi-Fi and LAN, to make last minute tweaks in his proposal. To his horror he finds all his files gone. The hard drive of his laptop had been wiped clean with just one file sitting in there titled, "Gothcha!" Brian obviously had to postpone his call with the client which he knew did not go down well. He called the network admin of FNB to take a look at his computer. To his surprise the network admin informed him that this was something that employees of FNB were facing throughout the world.

Computers of FNB employees around the world were systematically being victimized by rampant hacking. The hacking was not only widespread, but was being executed so flawlessly that the attackers, after compromising a system, stole everything of value and completely erased their tracks within 20 minutes.

Brian immediately brought this to the notice of the top management. Understandably they were concerned about their network and the reputation of their organization. The sheer volume of systems hacked was an alarming revelation for them.

The management has decided to seek the service of a penetration tester or security auditor to audit their networks for security vulnerabilities in order to avoid future attacks.

FNB has identified you as a third-party penetration tester to perform the pen testing of their information infrastructure. Your challenge is to perform a thorough pen test so that people like Brian don't have to cancel their business calls in future.

EC-Council

101 C Sun Ave NE
Albuquerque, NM 87109
http://www.eccouncil.org
Email: ecsaexam@eccouncil.org

Hackers are here. Where are you?